Remarks

Reconsideration of the application and allowance of all pending claims are respectfully requested. Claims 1-20 remain pending.

In the Office Action, claims 1, 4, 6, 8, 12-15, 17, 18 & 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret et al. (U.S. Patent No. 5,923,884; hereinafter Peyret) in view of Chen et al. (U.S. Patent No. 6,360,364 B1; hereinafter Chen) and further in view of Zumkehr et al. (U.S. Patent No. 5,974,529; hereinafter Zumkehr), while claims 2, 7, 10 & 19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Chen, and further in view of Zumkehr, and further in view of Everett (U.S. Patent No. 6,575,372 B1; hereinafter Everett), claim 16 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Chen, and further in view of Zumkehr, and further in view of Hänel (UK Patent Application No. GB 2314948 A; hereinafter Hänel), claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Chen, and further in view of Zumkehr, and further in view of Klingman (U.S. Patent No. 5,729,594; hereinafter Klingman), and claim 9 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peyret in view of Chen, and further in view of Zumkehr, and further in view of a textbook by B. Schneier entitled, "Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code NC" (hereinafter, Schneier). Each of these rejections is respectfully, but most strenuously, traversed and reconsideration thereof is requested.

Applicants request reconsideration and withdrawal of the obviousness rejection on the following grounds: (1) the Office Action has misinterpreted the teachings of Chen, thus voiding the basis for the rejection of the independent claims; (2) the combination of documents fails to disclose Applicants' claimed invention; (3) the basis for the combination of the documents set forth in the Office Action is deficient; (4) the documents themselves lack any teaching, suggestion or incentive for their further modifications as necessary to achieve Applicants' recited invention; and (5) the combination, to the extent characterized in the Office Action, is a hindsight reconstruction of the claimed invention using Applicants' own disclosed subject matter.

As set forth at page 2 of the specification, Applicants note that the widespread use of distributed systems has resulted in an ever-increasing need for downloading of on-card application components to a chipcard via the distributed systems. The risks of such methods are many. The network is subject to varying loads, so the download may take a long time depending on capacity. Another key aspect in this context is security. All data transferred from the server via a client to the chipcard should be safeguarded. Further, it must be ensured that a simple, secure authentication and encryption technique which responds to the varying loads on the network is used when downloading application components. The present invention is directed to addressing these needs.

Independent claims 1, 17 & 20 recite a method, device and computer program product, respectively, which implements a protocol for downloading application components from a server via a client to a chipcard. This protocol includes: delivering a secret key or Session Key by the sever to the client; loading into the server a sequence of commands to download an application component to the chipcard; generating a digital signature in the server using the secret key or Session Key by way of each command within the command sequence; transmitting the signed command sequence as a data packet to the client; unpacking of the data packet by the client and transmission of individual commands of the packet in sequence to the chipcard; and then checking the digital signature of the individual commands on the chipcard and executing the commands if the digital signature is correct.

In accordance with Applicants' protocol, downloading of application components is divided into stages. The first stage occurs only on the server, which ensures that not every command to download the application component is sent individually over the network connecting the server and client. This is achieved by an optimization protocol which bundles the individual commands to download the application component into a command sequence and then sends this command sequence as a data packet over the network. This reduces the time required for downloading application components over the network. In accordance with Applicants' protocol, each command within the command sequence is assigned a digital signature, and where appropriate, encrypted. This assures that only authenticated commands are accepted by the chipcard. Thus, the protocol meets security requirements for the transferred data via distributed systems, such as over the Internet.

The second stage occurs between the client and the chipcard and ensures that the data packet is unpacked and sent individually to the chipcard. The individual commands of the unpacked data packet are sent sequentially to the chipcard from the client. Thus, in accordance with Applicants' invention, intelligence is added to the client for receiving a data packet comprising a signed command sequence, and then unpacking the data packet and transmitting the individual commands in sequence to the chipcard. Independent claim 18 focuses on this aspect of Applicants' protocol, wherein a client is provided with the intelligence via a computer program product to execute the unpacking of the data packet comprising the signed command sequence and then transmit the individual commands thereof in sequence to the chipcard.

Applicants respectfully submit that the above-summarized protocol is simply not taught or suggested by the art of record, and in particular, by the applied documents.

Peyret discloses a system and method for loading applications onto a smartcard. FIG. 4 depicts a block diagram showing a system in accordance with Peyret's invention for loading an applet having use rights into a smart card. The system may include the smart card 20, a terminal 80, and a server 82. The smart card may have an interface system 86 that may connect the smartcard to the terminal 80 using a corresponding interface 88. A second interface 90 may connect the terminal to the server 82 via interface 92. Thus, the smartcard may be connected, through the terminal, to the server.

A method of loading an application into the smartcard is described at Col. 7, line 43 – Col. 8, line 15 of Peyret. As described, an application is loaded from server 82 to smart card 20 via the terminal. However, in the embodiment described by Peyret, terminal 80 simply comprises a pass-through or dumb terminal since there is no intelligent protocol at terminal 80 which facilitates the loading of the application from the server to the card. Peyret in fact describes the traditional prior art approach to downloading an application to a smartcard and hence has the disadvantages noted by Applicants in their Background of the Invention section of the specification.

Applicants respectfully submit that a careful reading of Peyret fails to disclose any teaching or suggestion of various aspects of their protocol for downloading application components from a server via a client to a chipcard. For example, Peyret does not teach or suggest any processing protocol between the sever and terminal (i.e., client) which would minimize data transfers between the server and the client. Further, there is no teaching or suggestion in Peyret that the terminal described therein is even able to read the content of the messages from the server. Rather, the Peyret terminal is simply a pass-through terminal. Peyret does not introduce the concept of transmitting a signed command sequence as a data packet from a sever to the client as recited by Applicants, nor the unpacking of the data packet by the client and then the transmission of individual commands within the packet in a sequence to the chipcard.

The Office Action recognizes certain of the above-noted deficiencies of Peyret when applied against Applicants' independent claims. Specifically, at page 3, line 19, the Office Action recognizes that Peyret does not disclose that the application is unpacked at the user terminal before being installed on the smart card; however, Chen is cited as allegedly disclosing this aspect of Applicants' claimed process. This conclusion is respectfully traversed. The conclusion is believed based on a mischaracterization of the Chen teachings at column 8, line 66 – column 9, line 22 (cited in the Office Action).

Chen describes a system and method for installing an application on a portable computer. One embodiment of the portable computer is depicted in Fig. 3 of Chen. The term "portable" is used in Chen to indicate a small computing device having a processing unit that is capable of running one or more application programs, a display, and an input mechanism that is typically other than a full-size keyboard. The input mechanism may be a keypad, touch-sensitive screen, trackball, touch-sensitive pad, miniaturized QWERTY keyboard, or the like. (See column 7, lines 17-25 of Chen). Figure 4 of Chen is a block diagram illustrating pertinent components of a portable computer, while Fig. 5 is an architectural diagram of a system for installing an application on a portable computer.

Initially, Applicants note that Chen does not describe a chipcard or smart card as the term is understood in the art and employed in the present application. The portable computer of Chen is a different device, with different components than that of a chipcard. Thus, Applicants respectfully traverse any extrapolation of the teachings of Chen for application to a chipcard environment as recited in their pending claims.

Further, as noted above, the Office Action references column 8, line 66 – column 9, line 22 for allegedly disclosing a feature of Applicants' claimed process, i.e., the process of unpacking a data packet by the client and transmitting individual commands from the data packet in sequence to the chipcard. However, as noted above, this conclusion is believed based on a misinterpretation of Chen. In Chen, the desktop application manager module 106 copies the CAB files into built-in memory 110 on the portable computer, or into one of the attached memory expansion cards 112. Once the CAB files are copied into built-in memory 110 or expansion card 112, the load module 226 is invoked to install the CAB file components into built-in memory 110 or into memory expansion card 112, as appropriate. This load module unpacks the CAB file and installs the application directly to the memory 110 or expansion card 112. As shown in Figs. 4 & 5 of Chen, the load module and this unpacking occurs within the portable computer itself. Thus, not only is there no chipcard described or depicted in Chen, but further, the portable computer to which the chipcard is analogized is actually performing the unpacking of the CAB files copied into its memory. Thus, no analogous processing is occurring in Chen to that recited by Applicants. In Applicants' claimed invention, their process includes the step of unpacking of the data packet by the client, and transmission of the individual commands from the packet in sequence to the chipcard. Thus, Applicants respectfully submit that the cited lines of Chen simply do not teach or suggest the recited functionality at issue in their independent claims.

To summarize, Chen does not teach or suggest receipt of a data packet at a client comprising a sequence of signed commands to then be forwarded to a chipcard, nor does Chen describe the unpacking of this data packet by the client and transmission of the individual commands in sequence to the chipcard. There is no chipcard *per se* in Chen, nor is there any unpacking of a data packet by a client, or the forwarding of individual commands from the client to the chipcard. As noted above, the unloading described by Chen at column 9, lines 1-22

(referenced in the Office Action) refers to the portable computer unpacking the CAB file that was downloaded to its memory from the desktop application manager module, which processing is clearly distinct from that recited by Applicants. For at least these reasons, Applicants respectfully submit that the Office Action has mischaracterized the teachings of Chen in alleging that Chen teaches the aspect of their process at issue, and in alleging that the combination of Peyret and Chen discloses the various steps of Applicants' claimed invention noted above.

Further, Applicants respectfully traverse the combinability of Chen and Peyret as alleged in the Office Action. The Office Action alleges that: "It would have been obvious to one of ordinary skill in the art at the time the invention was made to unpack the application program of Peyret on the user terminal before transferring the application to the smart card in order to minimize the decisions required of a user when installing an application as taught by Chen (column 9, lines 24-26)." (Emphasis added.)

Applicants respectfully submit that the rationale for combining Chen and Peyret of the Office Action is deficient. The basis for the deficiency arises from the difference between a portable computer and a chipcard as recited by Applicants (or smart card as described by Peyret). In a chipcard or smart card, there is no display, or user input device that would allow the user to make decisions via the chipcard. Fig. 1 of Peyret depicts one example of a smart card (or chipcard) which includes a CPU 22, and various memories 26, 28 & 30. As noted above, Chen discloses a portable computer that receives cabinet files from a desktop manager, and which has a display and an input mechanism (see column 7, lines 17-32). Thus, at column 9, lines 24-26, the procedure of Figure 6 of Chen cited in the Office Action seeks to minimize decisions required of a user when installing applications to the portable computer. These decisions would be input by the user via the portable computer. Since there is no input or interface capability on a chipcard or smart card, the rationale for extracting the teachings of Chen in a portable computer environment and applying those teachings to Applicants' chipcard environment is believed deficient. Minimizing decisions required of a user is not relevant to the claimed functionality of Applicants' process. Rather, as noted above, Applicants' invention is directed, in part, to a secure method which minimizes loading on a network, and which efficiently downloads application components to a chipcard.

For the above reasons, Applicants respectfully submit that the combination of Peyret and Chen would not have taught one skilled in the art their claimed functionality for digitally signing each command of a sequence at a server, transmitting the signed command sequence as a data packet to the client, and then unpacking of the data packet by the client, and transmission of the individual commands in sequence to a chipcard. The Office Action further cites Zumkehr for disclosing a system for error detection wherein individual program instructions are digitally signed and later authenticated. Without acquiescing to this characterization of the teachings of Zumkehr, Applicants note that Zumkehr does not teach or suggest the above-noted deficiencies of Peyret and Chen when applied against their independent claims.

Still further, upon a review of the applied patents, there is no teaching, suggestion or incentive for a further modification of the combination as would be necessary to achieve Applicants' invention. The portable computer of Chen does not comprise a chipcard, nor smart card, and the particular unloading process described therein does not teach or suggest Applicants' technique wherein intelligence is provided at a client for unpacking a data packet that has a signed command sequence, and then the transmission of the individual commands in sequence to the chipcard.

Yet further, the characterizations of the teachings of Peyret and Chen stated in the Office Action provide no technical basis outside that contained in Applicants' own specification. The characterizations of the teachings of Chen in particular merely assert the language of Applicants' claimed invention in hindsight, and notwithstanding that the patent actually teaches a different process. Thus, the rejection violates the well-known principle that Applicants' own disclosure cannot be used as a reference against them.

The consistent criterion for a determination of obviousness is whether the art would have suggested to one of ordinary skill in the art that the claimed invention should be carried out and would have a reasonable likelihood of success, viewed in light of the prior art. The suggestion and the expectation of success must be found in the prior art, not in the Applicants' disclosure. In re Dow Chemical Company, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1998) (multiple citations omitted). The alleged combination at issue is in part characterized in the language of Applicants' own disclosure, rather than an identified basis in the prior art for achieving the modifications

necessary to arrive at Applicants' claimed invention, in violation of this well-known principle. This yet another, independent reason why the current invention is not obvious over the applied art.

In summary, Applicants traverse the rejection of the independent claims based upon the misinterpretation of the Peyret and Chen patents; the lack of a teaching or a suggestion of their invention in the combination; the lack of a basis for the combination alleged; the lack of an actual teaching, suggestion or incentive in the art for the modifications necessary to achieve their invention; and the use of Applicants' own disclosure and results as a basis for the alleged modifications.

For all the above reasons, Applicants respectfully submit that the independent claims patentably distinguish over the teachings of Peyret, Chen, and Zumkehr. Reconsideration and withdrawal of the obviousness rejection based thereon is therefore respectfully requested.

The dependent claims are allowable for the same reasons as the independent claims, as well as for their own additional characterizations. Everett, Hänel, Klingman and Schneier are each cited in the Office Action for allegedly teaching various aspects of Applicants' dependent claims. Without acquiescing to the characterization of these references and their alleged applicability to Applicants' dependent claims, Applicants note that none of the references are cited in the Office Action for teaching or suggesting Applicants' above-noted protocol for downloading application components from a server via an intelligent client to a chipcard.

For at least the above reasons, Applicants respectfully submit that all claims are in condition for allowance and such action is respectfully requested.

If a telephone conference would be of assistance in advancing prosecution of the subject application, Applicants' undersigned attorney invites the Examiner to telephone him at the number provided.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan, Esq.
Attorney for Applicants
Reg. No.: 31,789

Dated: February 14, 2005

HESLIN ROTHENBERG FARLEY & MESITI P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579